REMARKS

Claims 1-16, 18-29, 31, 32, 34 and 36 are pending in the application. Applicant, by this paper, amends claims 1, 9, 14, and 16. Applicant respectfully requests reconsideration and allowance of all pending claims.

DISCUSSION OF REJECTIONS UNDER 35 U.S.C. §112

Claims 16-22 were rejected under 35 U.S.C. §112, first paragraph, for inclusion of the term "non-specific hardware platform" in claim 16. The Examiner alleges that the term is not defined in the specification.

Claims 16-22 were also rejected under 35 U.S.C. §112, second paragraph, as indefinite for reciting the term "non-specific hardware platform" in claim 16.

Applicant believes that paragraph [1024] from the Specification previously cited in the response dated August 4, 2006 clearly shows that the term "non-specific hardware platform" was set forth and defined in the original application, as filed. However, Applicant amends claim 16 to remove the term that is the basis of the Examiner's rejections.

Claim 16 is amended to include " obtaining a second identifier for the hardware, the second identifier identifying a hardware platform." As set forth in paragraph [1024] from Applicant's Specification, as filed,:

> The hardware is similarly assigned a hardware ID, which may be a model number, a product number, and so on. Each different hardware platform is assigned a different hardware ID, but all instances or units of the same hardware platform have the same hardware ID. Similarly, each software release is assigned a different software ID, but all instances or copies of the same software release have the same software ID. *The software ID and hardware ID thus identify the software release and hardware platform, respectively, and not specific instances of the software and hardware*. (*emphasis added*).

Applicant respectfully requests withdrawal of the rejections under 35 U.S.C. §112 in light of the claim amendments.

DISCUSSION OF REJECTIONS UNDER 35 U.S.C. §103

Claims 16, 18, and 21-22 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 6,243,468 to Pearce et al. (hereinafter Pearce) in view of U.S. Patent No. 6,931,545 to Ta et al. (hereinafter Ta). Claims 1-15, 19, 20, 23-29, 31, 32 and 34 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over Pearce in view of Ta, in further view of pages 303-307 of "How The Internet Works" by Gralla (hereinafter Gralla).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be reasonable expectation of success. Finally, the prior art reference, or references when combined, must teach or suggest all of the claim limitations.

The references cited by the Examiner, whether alone or in combination, fail to teach or suggest every limitation of the claims. Additionally, there is no motivation to combine or modify the references in the manner suggested by the Examiner.

Claim 16 includes "obtaining a second identifier for the hardware, the second identifier identifying a hardware platform." As expressly explained in Applicant's Specification, at page 4, paragraph [1024] ("Each different hardware platform is assigned a different hardware ID, but all instances or units of the same hardware platform have the same hardware ID....The software ID and *hardware ID thus identify the software release and hardware platform*, respectively, and n*ot specific instances of the software and hardware*.") (*emphasis added*).

Applicant's Specification clearly states that *the hardware ID identifies a hardware platform and not a specific instance of the hardware.*

In direct contrast to Applicant's claimed second identifier identifying a hardware platform, Pearce describes a hardware identifier that is used to identify a *specific instance* of a computer on which software is installed. For example, Pearce states: "The software product 100 generates a hardware ID (H/W ID) that identifies a set of hardware components that make up the customer's computer 32." *Pearce*, at Col. 5, ll. 57-59. "The anti-piracy system is effective at stopping repeated installation of the same software product on multiple different machines." *Id.*, at Col. 7, ll. 14-16. Pearce goes on to state: "If an unscrupulous customer attempts to install the product on another computer, the software product will determine the test and registration IDs do not match and will self lock." *Id.*, at ll. 31-34 (the test ID is generated using the computer specific hardware ID).

Thus, instead of permitting installation of software on any instance of a hardware platform, Pearce identifies each specific instance of hardware with a different hardware ID to explicitly forbid such installation.

Further, Pearce cannot be modified to operate with a hardware ID that identifies a hardware platform that is common to many instances of the hardware, because modifying Pearce in such a manner would render Pearce's system unsuitable for its intended purpose.

Claim 16 also includes the feature " receiving a digest obtained by hashing the software, and wherein the first signature is generated over the digest, the first identifier, and the second identifier." This claimed feature is not taught nor suggested in either Pearce or Ta.

The Examiner concedes that Pearce fails to teach or suggest using a hash of the software. *See, Office Action*, dated October 19, 2006, at page 3. However, the Examiner contends that "Ta discloses hashing software (creating a hash digest) to create a software ID to use in authenticating the software." *Id.*

In contrast, claim 16 features receiving the digest and generating the first signature over the digest, software ID (first identifier), and hardware ID (second identifier). Ta fails to teach or suggest receiving a digest and using the digest in generating a *signature*. Even if Ta describes using a hash digest to create a *software ID*, as argued by the Examiner, Ta fails to describe generating a signature for software based on the digest.

Applicant's claim 16 features generating the signature over both the digest and the software ID (first identifier). The Examiner merely identifies in Ta an alternative method of creating a software identifier.

Pearce and Ta, whether alone or in combination, fail to teach or suggest every feature of claim 16. Pearce cannot be modified to operate on a hardware identifier that identifies a hardware platform and not specific instances of hardware, because to do so would render Pearce unsuitable for its intended purpose. Additionally, neither Pearce nor Ta describes generating a signature over a digest, software ID, and hardware ID, and thus, the combination of the two references does not teach nor suggest a feature absent from each individually. Applicant respectfully requests reconsideration and allowance of claim 16.

Claim 1 features "authenticating a certificate from a code image with a first public key, the code image including the software." Support for this feature is found in Applicant's Specification, for example, at FIG. 2. Claim 1 also features " obtaining a signature generated for the software from the code image." Again, as shown in Applicant's FIG. 2, the signature (code signature) is part of the code image sent from the code generator entity to the wireless device.

None of the cited references teaches or suggests a code image having software and a certificate. As such, none of the cited references teaches or suggests authenticating a certificate from a code image with a first public key.

Pearce and Ta fail to describe a code image having a certificate and fail to describe authenticating any certificate that is part of a code image. The Examiner points to Gralla as teaching public key cryptography and digital certificates.

The Examiner contends that it would be obvious to use digital certificates and public key cryptography in Pearce's network to protect information and increase security. However, the Examiner provides no suggestion or motivation that would motivate one to implement the specific feature of including a certificate in a code image.

The mere fact that references *can* be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). The mere fact that communications can be made more secure does not provide sufficient motivation for one or ordinary skill in the art to make the specific modification of including a certificate with a code image or of authenticating a certificate from a code image.

Claim 1 also features "obtaining a signature generated for the software from the code image" and "validating the signature with a second public key from the certificate." Again, neither Pearce nor Ta describes a signature generated for software that is part of a code image. Furthermore, Gralla fails to mention adding any signature to a code image nor does Gralla teach or suggest validating a signature from a code image with a public key included in the certificate that is also part of the code image. Instead, Gralla describes adding a digital signature to accurately identify a *sender* of a message. Gralla fails to teach or suggest a signature that validates an association of software with hardware.

The Examiner argues that it would be obvious to use the techniques of Gralla to secure Pearce's network communication. However, Pearce fails to describe the software anti-piracy system as sending the software code over a network. Instead, Pearce describes the software product as communicating a software ID and a hardware ID generated from the computer on which it is installed. Pearce never describes sending the software code as part of the anti-piracy system. Therefore, there is nothing in the references themselves that teaches or suggests that including a signature with a code image or validating a signature from a code image with a public key would in any manner increase the security in validating software for hardware.

The Examiner argues that it would be obvious to include a signature in a code image that needs to be validated using a public key, but the cited references fail to describe any need for including a signature in a code image for the purposes of validating software for hardware.

Therefore, for this reason, independent of any reason discussed above, claim 1 is believed to be allowable, and Applicant respectfully requests reconsideration and allowance of claim 1.

Claim 9 includes a feature of a processor operative to authenticate a certificate from a code image and obtain a signature from a code image. Therefore, claim 9 is believed to be allowable at least for the reasons presented above in relation to claim 1.

Claim 14 includes the feature " means for authenticating a certificate sent with a code image including the software," and " means for obtaining a signature generated for the software and sent with the code image." Therefore, claim 14 is believed to be allowable at least for the reasons presented above in relation to claim 1.

Claim 23 includes the feature " a communication unit operative to obtain, from a code generator entity, information for a software code, a first identifier for the software, and a second identifier for the hardware." This feature is not taught nor suggested by the cited references, whether alone or in combination.

The Examiner fails to cite any reference that teaches or suggests the claimed feature, but instead, argues that the combination of Pearce, Ta, and Gralla teaches or suggests the claimed feature. It is error to reconstruct the claimed invention from the prior art by using the claim as a "blueprint." When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985).

Pearce fails to describe obtaining an identifier for hardware *from a code generator entity*. Instead, Pearce describes the software itself generating a hardware identifier that is unique to the hardware components that make up the computer on which the software is installed. *See, Pearce*, at Col. 5, ll. 57-59.

Pearce is concerned with permitting initial software on any hardware and limiting subsequent installations of the same software onto other hardware. The code generator entity in Pearce cannot distribute the hardware ID, because the hardware ID in Pearce is unique to the computer on which the software is installed. It would not be possible for the code generator entity to know the hardware ID of a user's computer, such that it could be included with the software. Indeed, Pearce cannot be modified to permit the code generator entity to include or have knowledge of the hardware ID because this would defeat the very anti-piracy techniques described in Pearce, thus rendering Pearce unsuitable for its intended purpose.

Claim 23 is believed to be allowable because the references, whether alone or in combination, fail to teach or suggest all features of the claim. Applicant respectfully request reconsideration and allowance of claim 23.

Claim 27 includes "means for generating a first signature for the software, based on the digest, the first identifier, and the second identifier using cryptography and a first secure cryptographic key, wherein the first signature is used to validate an association of the software with the hardware." At least this feature is absent from the cited references, whether alone or in combination. Indeed, the Examiner fails to provide any basis for a rejection of this claim, other than a general conclusion that the combination of references teaches all of the claimed features.

The Examiner concedes that Pearce and Ta, whether alone or in combination, fail to teach or suggest public keys or a certificate. *See, Office Action*, at page 4. The Examiner contends that because Gralla describes secure network communications, the combination of Gralla with Pearce and Ta teaches or suggests every claimed limitation. Applicant respectfully traverses the rejection.

None of the cited references, whether alone or in combination, teaches or suggests generating an encrypted signature to validate an association of the software with the hardware. Pearce and Ta fail to teach or suggest any use of public keys for validating an association of the software with the hardware. Gralla describes public key encryption for authenticating senders of a message, and fails to mention any validation of software with hardware. There is nothing in secure network communications to even suggest that public key cryptography could be used in validating software for hardware.

Thus, the cited references, whether alone or in combination, fail to teach or suggest every claimed feature. Application respectfully requests reconsideration and allowance of claim 27.

Claim 29 includes the features of "receiving a signature generated for the software, the first identifier, and the second identifier, wherein the signature is generated using cryptography and a first secure cryptographic key, and is used to validate an association of the software with the hardware," and "receiving a certificate containing cryptographic information used to validate the signature, the certificate generated using cryptography and a second secure cryptographic key." This combination of features is neither taught nor suggested by the cited references, whether alone or in combination.

The cited references fail to teach or suggest an encrypted signature, as described above in relation to claim 27. Additionally, as described above in relation to claim 27, the cited references fail to teach or suggest using a certificate to validate a signature that associates software with hardware. The Examiner concedes that Pearce and Ta fail to describe certificates, and Gralla fails to describe a certificate that can be used to validate a signature that associates software with hardware.

Thus, the cited references, whether alone or in combination, fail to teach or suggest every claimed feature. Application respectfully traverse the rejection of claim 29 and requests reconsideration and allowance of claim 29.

Claims 32 and 34 include apparatus operative to perform the method of claim 29 and is believed to be allowable at least for the reasons presented above in relation to claim 29. Application respectfully requests reconsideration and allowance of claims 32 and 34.

DISCUSSION OF DEPENDENT CLAIMS

Claims 2-8, 10-13, 15, 18-22, 24-26, 28, and 31 depend from one of claims 1, 9, 14, 16, 23, 27, or 29 and are believed to be allowable at least for the reason that they depend from an allowable base claim. The Examiner fails to even provide any particular description as to how the combination of references purports to describe every feature of each of the dependent claims. Thus, the Examiner fails to establish a *prima facie* case of rejection for the majority of the dependent claims. Applicant requests reconsideration and allowance of claims 2-8, 10-13, 15, 18-22, 24-26, 28, and 31.

Each of the dependent claims may have independent basis for patentability distinct from those discussed in relation to the independent claims. Although it is not necessary for Applicant to discuss the independent basis for patentability, Applicant provides some illustrative examples.

Claims 3, 10, and 15, include features, generally, of hashing software information, software ID information and hardware ID information to obtain a first digest. The claims further include features of decrypting a signature that is part of the code image to generate a second digest. The two digests are compared to validate the signature. None of the cited references teaches or suggests this combination of claimed features. Indeed, the Examiner fails to cite any portion of the references that teaches or suggests the claimed features or the combination of features.

Claims 5, 18, and 31 explicitly feature HMAC. Applicant's Specification, at paragraph [1039] describes HMAC as described in the public document RFC 2104. None of the cited references teaches or suggests using HMAC. Indeed, none of the cited references even mentions HMAC.

Claim 11 includes the feature that a storage unit store boot code to authenticate the certificate and validate the signature. This feature is not taught nor suggested in any of the cited references. Pearce explicitly describes the software itself as performing the anti-piracy technique. Pearce cannot be modified to include boot code that performs the process, because the boot code could not possibly know what software will be added to the computer, and thus cannot include boot code that authenticates certificates or validates a signature.

Applicant reiterates that the discussion of dependent claims is solely illustrative of the patentable features in the dependent claims. The discussion of dependent claims is not intended to be exhaustive of the patentable features in the dependent claims.

DISCUSSION OF NEW CLAIM

Applicant adds new claim 36. Support for the claim can be found in Applicant's Specification, as filed. In particular, support can be found at FIGs. 8-10, and the associated description at paragraphs [1049] through [1064].

The combination of claimed features in neither taught nor suggested by the cited references, whether alone or in combination. In particular, none of the cited references describes a secure storage device that stores a hardware identifier and a certificate authority public key.

Applicant respectfully requests allowance of new claim 36.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the Application are patentable. Accordingly, reconsideration and allowance of this Application is earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

If there are any fees due in connection with the filing of this response, please charge such fees to our Deposit Account No. 17-0026. If a fee is required for an extension of time under 37 C.F.R. 1.136 not accounted for, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully submitted,

/Howard H. Seo/

Dated: 2/20/07 By: ______________________

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502

Howard H. Seo
Registration No. 43,106
(858) 845-5235